00/8119
ISR 5/13/1 (a)

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000029841 A**

(43) Date of publication of application: **28 . 01 . 00**

(51) Int. Cl **G06F 15/00**
H04L 9/32

(21) Application number: **10199228**

(22) Date of filing: **14 . 07 . 98**

(71) Applicant: **IBIX KK**

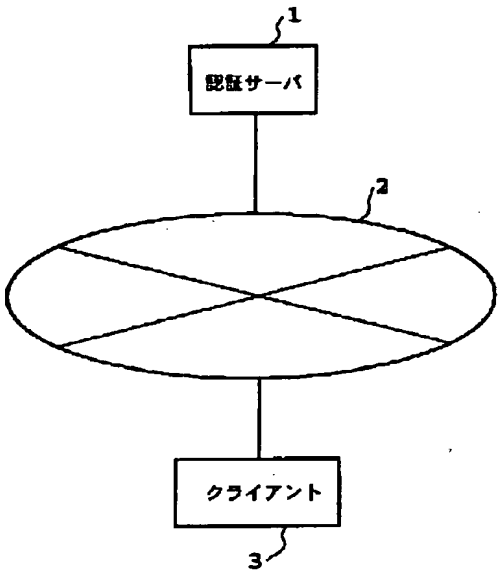
(72) Inventor: **ADACHI HIDEYUKI**

(54) **IMPERSONATION PREVENTION METHOD/DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To block the reception of an authentication certificate by an impersonator by collating communication records stored in both authentication server and client in the authentication server and/or the client in the case that an access request from the client is present.

SOLUTION: At the time of passing the authentication of individual information between the authentication server 1 and the client 3, the authentication server 1 issues the authentication certificate to the client 3. Also, the present date and time and the number of times of communication are written in a storage device inside the client 3 and the same date and time and number of times of the communication are preserved and stored also in the storage device inside the authentication server 1. In the case that a normal user accesses the authentication server 1 for second and succeeding times, a normal password is used. The authentication server 1 confirms that a user ID and the password are normal and the communication log of a previous time preserved inside the client 3 matches with the one preserved inside the authentication server 1 and permits transition to an authentication processing.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－29841
（P2000－29841A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｋ０１３

審査請求　有　　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願平10－199228

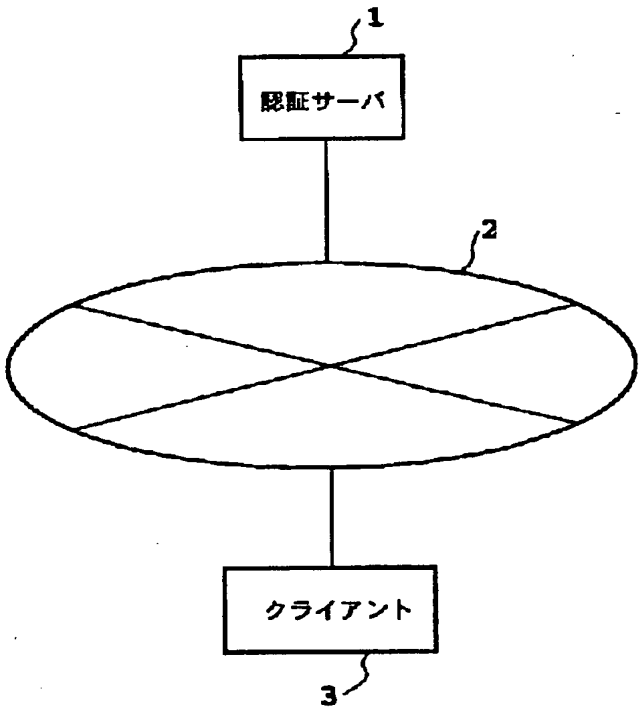
(22)出願日　平成10年７月14日(1998.7.14)

(71)出願人　595091366
アイピックス株式会社
東京都中野区弥生町４丁目34番８号
(72)発明者　足立　秀行
東京都中野区弥生町４－34－８　アイピックス株式会社内
(74)代理人　100077481
弁理士　谷　義一　（外３名）

Ｆターム(参考)　5B085 AC03 AE03 AE06 AE23 BG07
5K013 AA00 AA03 GA02

(54)【発明の名称】　なりすまし防止方法および装置

(57)【要約】
【課題】　認証処理のセキュリティ性を高める。
【解決手段】　認証サーバ１およびクライアント３の双方に通信記録を保存し、前回の通信記録の照合を行うことにより、不正アクセスを検知する。



1

【特許請求の範囲】
【請求項１】　認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止方法において、
前記クライアントおよび前記認証サーバの双方に同じ内容の通信記録をアクセス毎に記憶しておき、
前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を前記認証サーバおよび／または前記クライアントにおいて行って、
照合において一致判定が得られた場合には認証処理への移行を許可することを特徴とするなりすまし防止方法。
【請求項２】　請求項１に記載のなりすまし防止方法において、正規ユーザに対しては初回のアクセス時に使用する第１のパスワードおよび２回目以降に使用する第２のパスワードが通知されており、前記認証サーバおよび／またはクライアントは当該入力されたパスワードの照合を行って、該照合の結果に応じて前記認証サーバにおける認証処理への移行を許可することを特徴とするなりすまし防止方法。
【請求項３】　認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止装置において、
前記クライアントおよび前記認証サーバの双方に同じ内容の通信記録をアクセス毎に記憶しておき、
前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を行う通信記録照合手段と、
当該照合において一致判定が得られた場合には認証処理への移行を許可する制御手段とを具えたことを特徴とするなりすまし防止装置。
【請求項４】　請求項３に記載のなりすまし防止装置において、正規ユーザに対しては初回のアクセス時に使用する第１のパスワードおよび２回目以降に使用する第２のパスワードが通知されており、前記認証サーバには当該第１のパスワードと第２のパスワードと同じパスワードが記録されており、前記クライアントから入力されたパスワードおよび前記認証サーバに記憶されたパスワードの照合を行うパスワード照合手段をさらに有し、前記制御手段は、当該パスワードの照合の結果に応じて前記認証サーバにおける認証処理への移行を許可することを特徴とするなりすまし防止装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証サーバなどでクライアント側のユーザ認証を行う場合のなりすまし防止方法および装置に関する。

2

【０００２】
【従来の技術】世界的に開放されてきたインターネット等を介してオンラインショッピングが可能となってきている。インターネットのような通信ネットワークで商取引を行う場合に、当事者、たとえば、商品販売業者側では商品購入者が本人であるかの確認が必要となってくる。このような本人の認証のために認証サーバと呼ばれる第３者機関が認証を行う認証サービスシステムが提案されている。認証サーバでは、予めユーザ登録を受け付ける際に、ユーザがそのユーザのみが知りうる情報（以下、個人情報と称する）、たとえば、氏名、生年月日、住所等）をユーザから受け付け、認証サーバ内に保存しておく。ユーザに対しては、認証サーバにアクセスするためのパスワード、ユーザＩＤを引き渡す。本人認証が必要な場合に、ユーザは通信ネットワークに接続されたオンライン端末（クライアントとも呼ばれる）から上記ユーザＩＤおよびパスワードを使用して認証サーバにアクセスした後、個人情報を入力する。認証サーバでは、入力された個人情報と保存してある個人情報とを照合し、一致した場合にのみ、本人であることを証明する証明書（認証承認とも呼ばれる）を発行し、アクセスしてきたオンライン端末に証明書を送信する。オンライン端末側のユーザは、受信した証明書を、商品販売サービスを行うサーバに提示することにより本人であることの証明を行う。このような認証システムでは、商品販売サービスを行うものが、ユーザの認証のための個人情報を保存する必要がないというメリットと、ユーザ側にとっては、認証サーバにのみ個人情報を登録しておけばよく、多数の商品販売業者に対して、個人情報を公開しなくともよいというメリットがある。
【０００３】上記パスワードを保護するためにＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｒｓ　Ｌａｙｅｒ　Ｐｒｏｔｏｃｏｌ）のような通信プロトコルでは、送信データを暗号化する層を設けて、パスワードを暗号化して送信している。
【０００４】また、認証サーバが発行する証明書についてもデジタル署名や電子的すかしとよばれる方法で特定の情報を証明書に埋め込み、証明書の真偽を確認することができるようになっている。
【０００５】
【発明が解決しようとする課題】しかしながら、認証サーバへの登録者がユーザＩＤ、パスワード、個人情報を記載したメモを落としたり、他人に見られた場合、あるいは、暗号化されたこれらの情報をインターネット上で盗聴され、解読された場合、こららの情報を取得したものは本人になりすまして、個人認証を受け取ることができてしまう。
【０００６】そこで、本発明の目的は、上述の点に鑑みて、上述のようなりすまし者による認証証明書の受領

を阻止することができるなりすまし防止方法および装置を提供することにある。

【０００７】

【課題を解決するための手段】このような目的を達成するために、請求項１の発明は、認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止方法において、前記クライアントおよび前記認証サーバの双方に同じ内容の通信記録をアクセス毎に記憶しておき、前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を前記認証サーバおよび／または前記クライアントにおいて行って、照合において一致判定が得られた場合には認証処理への移行を許可することを特徴とする。

【０００８】請求項２の発明は、請求項１に記載のなりすまし防止方法において、正規ユーザに対しては初回のアクセス時に使用する第１のパスワードおよび２回目以降に使用する第２のパスワードが通知されており、前記認証サーバおよび／またはクライアントは当該入力されたパスワードの照合を行って、該照合の結果に応じて前記認証サーバにおける認証処理への移行を許可することを特徴とする。

【０００９】請求項３の発明は、認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止装置において、前記クライアントおよび前記認証サーバの双方に同じ内容の通信記録をアクセス毎に記憶しておき、前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を行う通信記録照合手段と、当該照合において一致判定が得られた場合には認証処理への移行を許可する制御手段とを具えたことを特徴とする。

【００１０】請求項４の発明は、請求項３に記載のなりすまし防止装置において、正規ユーザに対しては初回のアクセス時に使用する第１のパスワードおよび２回目以降に使用する第２のパスワードが通知されており、前記認証サーバには当該第１のパスワードと第２のパスワードと同じパスワードが記録されており、前記クライアントから入力されたパスワードおよび前記認証サーバに記憶されたパスワードの照合を行うパスワード照合手段をさらに有し、前記制御手段は、当該パスワードの照合の結果に応じて前記認証サーバにおける認証処理への移行を許可することを特徴とする。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。

【００１２】図１は本発明を適用した認証システムのシステム構成を示す。図１において、１は後述の認証を行い、認証合格者に対して認証証明書を発行する認証サーバである。２は公開された通信ネットワークである。３は認証を受けようとするユーザが使用するクライアントである。なお、インターネットのような通信ネットワークの場合には、通信ネットワーク２内にプロバイダと呼ばれる通信ネットワーク接続業者が存在し、プロバイダのゲートウェイを介してクライアント３を通信ネットワーク２に接続することが可能である。また、クライアント３が専用電話回線を使用して通信ネットワーク２に接続する場合もある。

【００１３】このようなシステム構成において、認証サーバ１は図に示す処理プログラムを実行して認証を行うとともに、なりすまし者（不正アクセス者）のアクセスを検知する。

【００１４】また、個人情報を登録した正規ユーザに対してはユーザＩＤおよびパスワードが書面で認証サービス会社から通知され、認証サーバ１に保存されているものとする。パスワードには初回のアクセスにのみ有効なパスワード（初期パスワードと称する）と、２回目以降のアクセスに使用するパスワード通常パスワードと称する）との２種類の異なるパスワードが正規ユーザに通知される。

【００１５】以下、図２を参照して、本発明に係る認証処理を説明する。本実施形態では、サーバ１および通信記録（ログと呼ばれる）をアクセス毎に保存しておき、認証サーバ１（クライアント３側でも可能）双方の通信ログが一致した場合に、正規のユーザのアクセスと判断し、認証処理への移行を許可することに特徴がある。

【００１６】従来と同様にして、クライアント３からのアクセス要求を受け取ると（ステップＳ１０のＹＥＳ判定）、次にクライアント３からのユーザＩＤおよびパスワードの入力（手動あるいは自動入力）を受け付ける。初めて認証を受けようとするユーザは初期パスワードを使用する。この入力されたユーザＩＤおよび初期パスワードとサーバ１内に保存されたユーザＩＤおよび初期パスワードの照合により、サーバ１ではアクセス要求を行ったユーザの認証が初回であることを知ることができる（ステップＳ２０のＹＥＳ判定）。

【００１７】サーバ１とクライアント３との間では、個人情報の入力と照合による認証処理を行う（ステップＳ１００）。認証に合格（照合結果の一致判定、ステップＳ１１０のＹＥＳ判定）すると、サーバ１は認証証明書をクライアント３に対して発行する。また、クライアント３内の記憶装置、たとえば、ハードディスクに現在の日時および通信回数（この場合、数値１）を書き込むと共に、サーバ１内の記憶装置にも同じ日時および通信回数を保存記憶する（ステップＳ１２０）。なお、クライアント３自身がこれらの日時および通信回数を書き込ん

でもよい。

【００１８】認証処理に失敗した場合（ステップＳ１１０のＮＯ判定）には認証を拒否する旨のメッセージがクライアント３に送信される（ステップＳ１３０）。

【００１９】初回の認証は従来とほぼ同じ処理となるが、次回から使用されるパスワードが異なるので、仮になりすましによるアクセスが成功しても、次回は、パスワードチェック（ステップＳ２０におけるパスワード照合）によりなりすまし者のアクセスが撃退される。

【００２０】正規のユーザが２回目以降、認証サーバ１にアクセスする場合には、通常パスワードを使用する。認証サーバ１は、ユーザＩＤおよびパスワードが正規のものであること、かつ、クライアント３に保存された前回の通信ログ、すなわち、通信の日時と通信回数が認証サーバ１内に保存されたものと一致することを確認する（ステップＳ３０）と、ステップＳ４０の認証処理への移行を許可する。

【００２１】認証サーバ１は従来と同様の個人情報による認証を行って、認証合格の場合には認証証書を発行して通信記録を保存（日時および通信回数）し、認証に失敗した場合には、認証拒否のメッセージをクライアント３に送信する（ステップＳ４０→Ｓ１２０，Ｓ１３０）。

【００２２】以上、説明したように、本実施形態では、認証サーバ１およびクライアントに保存した通信ログを比較することにより、通信ログを有していないなりすまし者のアクセスを撃退できる。加えて、通信ログをもたない正規ユーザのアクセスに対しては、初回にのみ有効なパスワードを設定することにより、なりすまし者と正規のユーザとを識別することができる。

【００２３】上述の実施形態の他に次の形態を実施できる。

【００２４】１）認証サーバ１およびクライアントに保存されたパスワード、通信ログの照合は認証サーバ１だけでなく、クライアント３側で行なってもよい。この場合には、認証サービス会社から専用の通信ソフトを支給し、この通信ソフト内で通信ログおよびパスワードの照合を行う。これらの照合をクライアント３側で行う場合には、認証サーバ１からクライアントに対して照合用の通信記録およびパスワード情報が送信される。また、これらの照合は認証サーバ１のみ、クライアント３のみ、あるいは双方で行う等の各種のバリエーションがあるが適宜、好適な形態を選択すればよい。

【００２５】２）図２に示す認証処理については認証サーバ１あるいはクライアント３に搭載されたＣＰＵにより実行すればよいが、この認証処理を規定したプログラムはＣＤＲＯＭ，フロッピーディスク等の携帯用記録媒体から実装したり、認証サーバ１からクライアント３に対してダウンロードすることができる。

【００２６】これらプログラムの中の本発明にかかわる不正アクセス者の検知処理を実行するＣＰＵがなりすまし防止装置として機能する。

【００２７】３）クライアント３には、パーソナルコンピュータ、ワードプロセッサ、ワークステーション、携帯用端末、電子手帳等の通信機能を有する各種の情報処理装置を使用することができる。

【００２８】４）上述の初期パスワードについては使用の有効期限を設定することによりさらにセキュリティ性を高めることができる。

【００２９】

【発明の効果】以上、説明したように、請求項１，３の発明によれば、通信記録を有しない不正アクセス者（なりすまし者）のアクセスを検知することができるので、この種の不正アクセスを撃退でき、認証サービスのセキュリティ性をさらに高めることができる。

【００３０】請求項２、４の発明では、正規のユーザが使用するパスワードを初回アクセス用と２回目以降用と異ならせることにより。初回にアクセスし、通信記録を有しない正規のユーザと不正アクセス者を識別することができる。

【図面の簡単な説明】

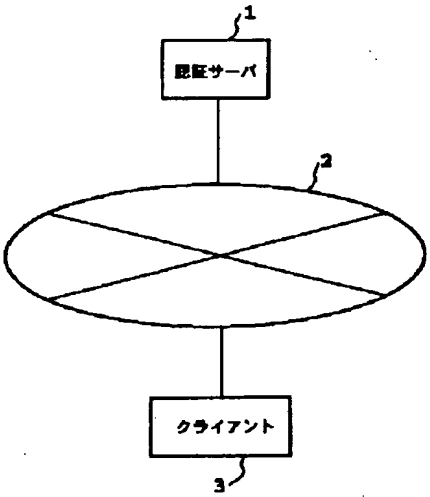
【図１】本発明実施形態のシステム構成を示すブロック図である。

【図２】図１の認証サーバ１の処理手順を示すフローチャートである。

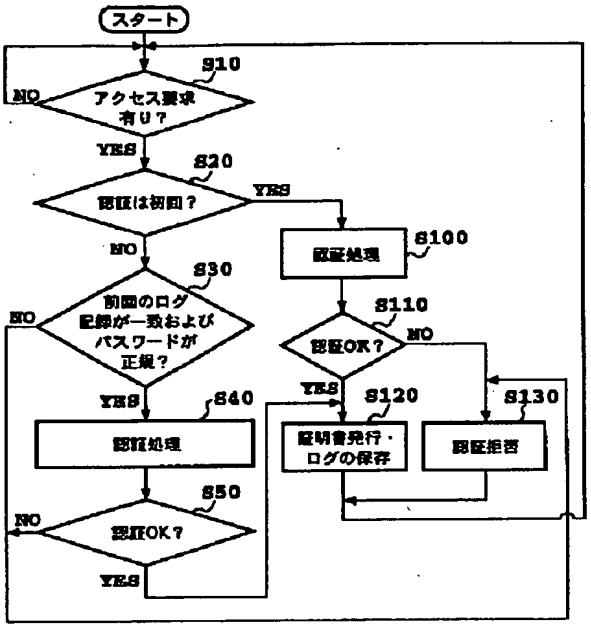
【符号の説明】

１　認証サーバ
２　通信ネットワーク
３　クライアント

【図１】



【図２】



【手続補正書】
【提出日】平成１１年６月２２日（１９９９．６．２２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項１
【補正方法】変更
【補正内容】
【請求項１】　認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止方法において、
前記クライアントおよび前記認証サーバの双方に、当該クライアントおよび認証サーバそれぞれが記録した同じ内容の通信記録をアクセス毎に記憶しておき、
前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を前記認証サーバおよび／または前記クライアントにおいて行って、
照合において一致判定が得られた場合には認証処理への移行を許可することを特徴とするなりすまし防止方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項３
【補正方法】変更
【補正内容】
【請求項３】　認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止装置において、
前記クライアントおよび前記認証サーバの双方に前記認証サーバの双方に、当該クライアントおよび認証サーバそれぞれが記録した同じ内容の通信記録をアクセス毎に記憶しておき、
前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を行う通信記録照合手段と、
当該照合において一致判定が得られた場合には認証処理への移行を許可する制御手段とを具えたことを特徴とするなりすまし防止装置。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正内容】
【０００７】
【課題を解決するための手段】このような目的を達成するために、請求項１の発明は、認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検

知するためのなりすまし防止方法において、前記クライアントおよび前記認証サーバの双方に、当該クライアントおよび認証サーバそれぞれが記録した同じ内容の通信記録をアクセス毎に記憶しておき、前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を前記認証サーバおよび／または前記クライアントにおいて行って、照合において一致判定が得られた場合には認証処理への移行を許可することを特徴とする。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正内容】

【０００９】請求項３の発明は、認証サーバに登録された情報とクライアント側から入力された情報との照合を行って、前記認証サーバから前記クライアントに対して認証証明書を発行する認証システムで不正アクセス者を検知するためのなりすまし防止装置において、前記クライアントおよび前記認証サーバの双方に前記認証サーバの双方に、当該クライアントおよび認証サーバそれぞれが記録した同じ内容の通信記録をアクセス毎に記憶しておき、前記クライアントからアクセス要求があった場合には、前記認証サーバおよび前記クライアントの双方に記憶された通信記録の照合を行う通信記録照合手段と、当該照合において一致判定が得られた場合には認証処理への移行を許可する制御手段とを具えたことを特徴とする。